Blockchain, Crypto Economy & NFTs

FS 2026

Learning Objectives

After this lecture you will be able to:

- Distinguish hot, warm, cold, MPC, and HSM custody architectures and their trade-offs
- Explain what a crypto prime broker does and which institutions offer which services
- Describe Real-World Asset (RWA) tokenisation and cite current market size evidence
- Analyse the BlackRock BUIDL and JPMorgan Kinexys case studies using the cryptoeconomics lens
- Evaluate whether a given institutional use case warrants on-chain settlement
- Apply Swiss regulatory context (FINMA, BVV2/OAK BV) to institutional digital-asset decisions

---

Estimated time: 45 min lecture + 15 min Swiss pension exercise

The Problem: Who Holds the Keys?

Custody is the core infrastructure problem:

- In traditional finance, custodians (BNY Mellon, State Street) hold assets in registered accounts
- In crypto, ownership = control of private keys
- A pension fund cannot leave $100M on a retail exchange wallet
- Institutional requirements: regulatory compliance, insurance, audit trail, SLAs

The institutional dilemma

"Not your keys, not your coins"

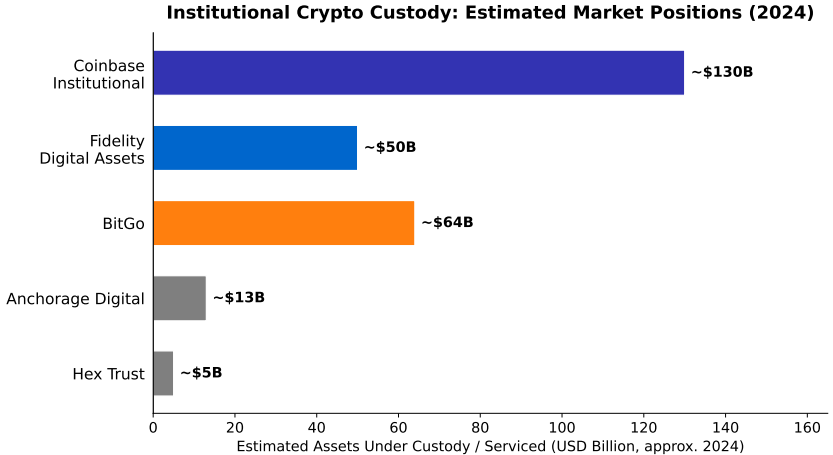
vs.

"Not your custodian, not your compliance"

Outcome: Specialised custodians emerged 2018-2022 solving exactly this tension.

FTX collapse (Nov 2022) accelerated institutional demand for segregated, audited custody.

The Institutional Custody Market (2024)



Note: Figures are approximate estimates from public disclosures and press reports.
Fireblocks (not shown) reports $1T+ in transaction volume, not AUM.

Coinbase Institutional: ∼$130B AUC (Coinbase 10-Q filings, 2024); BitGo: ∼$64B (BitGo press releases, mid-2024); Fidelity Digital Assets: ∼$50B (Fidelity institutional disclosures, 2024).

Custody Architectures: Hot, Warm, and Cold

Hot Wallet (Online)

- Keys live on internet-connected servers
- Instant transaction signing
- Highest attack surface
- Typical use: exchange operational float

Warm Wallet (Semi-online)

- Keys stored offline, brought online to sign
- Balance of speed and security
- Multi-sig approval required
- Typical use: day-to-day institutional flows

Cold Storage (Air-gapped)

- Keys never touch internet
- Hours to access
- Maximum security, insurable
- Typical use: long-term reserve holdings

Rule of thumb: most institutional custodians hold $>90\%$ of assets in cold storage, $<10\%$ warm/hot.

Separation of hot/warm/cold mirrors TradFi's settlement account hierarchy (nostro/vostro/reserve).

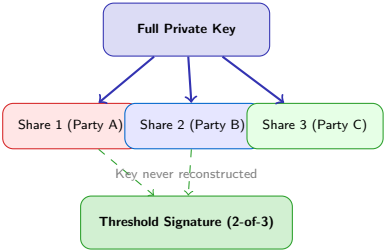
MPC: Multi-Party Computation Custody

What is MPC?

- Multi-Party Computation splits the private key into shares distributed across parties
- No single party ever reconstructs the full key
- Threshold signatures (e.g., 2-of-3) sign transactions without key assembly
- Eliminates single point of failure while maintaining operational speed

Who uses MPC?

- Fireblocks: MPC-based platform, $1T+ transaction volume reported
- Coinbase Advanced, BitGo Prime: MPC as default for institutional flows
- SIX Digital Exchange: MPC-secured settlement



MPC eliminates the "key ceremony" risk that plagued early Bitcoin corporate treasuries.

HSM: Hardware Security Modules

What is an HSM?

- Hardware Security Module (HSM): a FIPS 140-2 / FIPS 140-3 certified tamper-proof device
- Keys are generated and used inside the HSM; never exported in plaintext
- Physical tamper detection destroys key material if breached
- HSMs are the standard for TradFi (payment cards, PKI, banking cores)

HSM in crypto custody:

- Anchorage Digital: first US federally chartered crypto bank; HSM-based cold storage
- Fidelity Digital Assets: HSM-backed institutional custody since 2018
- SIX Digital Exchange: FINMA-regulated; HSM at core of settlement layer

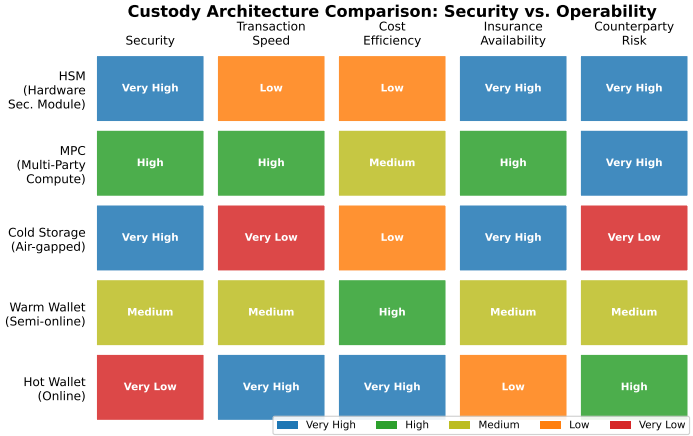
MPC vs. HSM: Key Distinction

MPC	HSM
Software-based	Hardware-based
Key split across nodes	Key sealed in device
Network-distributed	Physical device
Flexible geography	Specific location
Fireblocks model	Anchorage/SIX model

Many custodians combine both (HSM for root key, MPC for operational keys).

FIPS 140-3 (2019) is the current standard; FIPS 140-2 Level 3 still widely accepted for financial services.

Custody Architecture Comparison



MPC = Multi-Party Computation (key never reconstructed in one place). HSM = Hardware Security Module (FIPS 140-2/3 certified tamper-proof device).

MPC and HSM are not mutually exclusive: best-practice custodians use HSM for root key generation and MPC for operational signing.

What is a Crypto Prime Broker?

Prime brokerage in TradFi:

- Goldman Sachs, Morgan Stanley offer hedge funds: custody + leverage + execution + reporting
- Single counterparty for all capital-markets needs

Crypto prime brokerage (emerging 2020-2025):

- Custody of digital assets (segregated, audited)
- OTC trading (large block execution, low slippage)
- Margin lending against crypto collateral
- Derivatives (perpetuals, options, structured products)
- Staking services (yield on proof-of-stake assets)
- Reporting, tax, and compliance tooling

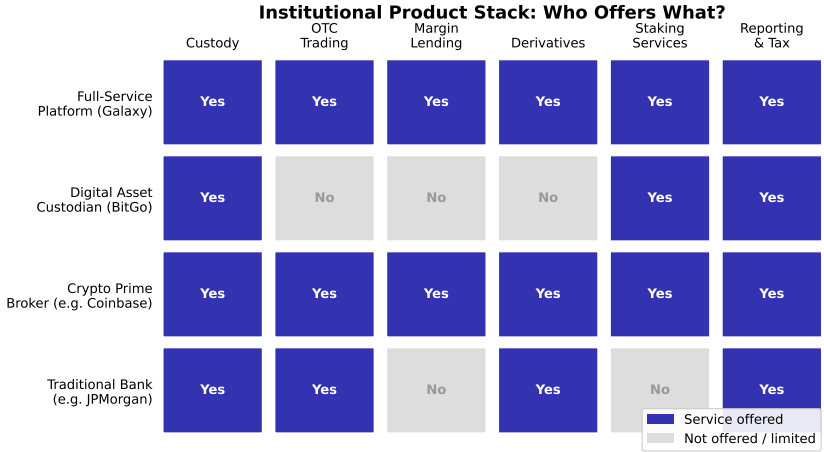
Why it matters for TradFi

Institutional investors will not interact with 5+ separate crypto venues. A prime broker provides:

- Single credit line
- Unified reporting
- Regulatory-grade counterparty
- Familiar workflow

FTX's collapse was partly a cautionary tale on the risks of "prime broker" without proper custody segregation.

Institutional Product Stack: Who Offers What?



Full-service platforms (Galaxy, Coinbase Institutional) approach TradFi prime broker capabilities. Traditional banks (JPMorgan) remain selective.

Who Uses Institutional Crypto Services?

Early adopters (2020-2022):

- Hedge funds: macro funds (Brevan Howard, Tudor Investment)
- Corporate treasuries: MicroStrategy, Tesla (brief), Block
- Family offices: private wealth seeking uncorrelated returns

2024-2025 entrants:

- Pension funds: Wisconsin Investment Board (BTC ETF)
- Sovereign wealth: Abu Dhabi, Norway (indirect via ETFs)
- Asset managers: BlackRock, Fidelity, Franklin Templeton on-chain funds

Catalyst: Bitcoin ETF approvals (Jan 2024)

- US spot Bitcoin ETFs approved January 11, 2024
- \$50B+ AUM within 12 months (as of 2024)
- Surpassed gold ETF AUM (Dec 2024)
- Enabled regulated exposure without self-custody

Key insight: ETFs de-risk adoption; tokenised funds (BUIDL, FOBXX) are the next step.

Wisconsin Investment Board disclosed BTC ETF holdings in May 2024 13-F filing: first US public pension to do so.

Real-World Asset Tokenisation: What and Why?

Definition:
Real-World Asset (RWA) tokenisation converts ownership rights of off-chain assets (bonds, equities, real estate, funds) into on-chain tokens.

Why now?

- Smart contracts automate settlement (T+0 vs. T+2)
- Programmable compliance (transfer restrictions encoded in token)
- 24/7 markets for traditionally illiquid assets
- Fractionalisation lowers minimum ticket sizes
- Interoperability across DeFi liquidity pools

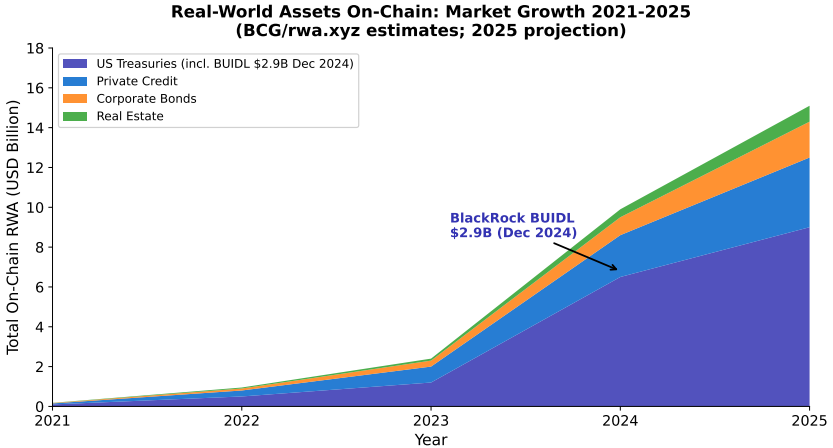
Asset categories on-chain (2025):

- **US Treasuries**: largest category (∼$9B)
- **Private credit**: Maple, Centrifuge (∼$3.5B)
- **Corporate bonds**: Siemens, EIB on-chain (∼$1.8B)
- **Real estate**: tokenised REITs, land registries (∼$0.8B)

Total on-chain RWA: ∼$15B deployed (early 2025, rwa.xyz)
Addressable market: $4T–$16T (BCG 2022 / Citi 2023 estimate)

Programmable compliance is the key institutional selling point: no manual transfer agent needed for know-your-customer checks.

RWA Market Growth 2021-2025



Note: Total on-chain RWA market estimated 4T−16T addressable (BCG 2022 / Citi 2023 range).
On-chain actual: ~$15B deployed as of early 2025 per rwa.xyz.

BlackRock BUIDL launched March 2024; reached $2.9B by December 2024, making it the largest tokenised treasury fund.

Case Study: BlackRock BUIDL

BlackRock USD Institutional Digital Liquidity (BUIDL)

- Launched: March 2024 on Ethereum (via Securitize)
- Structure: tokenised money-market fund (US Treasuries + repo)
- AUM: reached $2.9B (as of 2024) (Source: Securitize/BlackRock, Dec 2024)
- Minimum: $5M (institutional only)
- Yield: daily accrual, on-chain dividend distribution
- Redemption: T+0 via stablecoin (USDC) swap option

Why it matters:

- World's largest asset manager ($10T+ AUM) legitimises on-chain funds
- Provides DeFi protocols with yield-bearing "safe asset" collateral

BUIDL vs. Traditional MMF

	BUIDL	**TradFi MMF**
Settlement	T+0	T+1
Hours	24/7	Business hrs
Min. invest	$5M	$1M+
Composable	Yes	No
Custodian	Coinbase	TradFi bank
Regulator	SEC	SEC

BUIDL surpassed Franklin FOBXX to become the largest tokenised fund by AUM in May 2024.

Case Study: Franklin Templeton FOBXX

Franklin OnChain US Government Money Fund (FOBXX)

- Launched: 2021 on Stellar; expanded to Polygon 2023
- **First US-registered mutual fund** to use blockchain for record-keeping
- Assets: US government securities and repo agreements
- AUM: ∼$400-500M (2024; BUIDL surpassed it in May 2024)
- Ticker: BENJI (distributed via Benji Investments app)
- Min. investment: $20 (retail-accessible unlike BUIDL)

FOBXX significance

- Proved regulators (SEC) would accept blockchain share registrar
- Opened path for BUIDL, Ondo, Superstate and others
- Demonstrated Stellar as institutional settlement layer
- Cross-chain expansion shows portability demand

FOBXX = Franklin OnChain US Government Money Fund. "Onchain" in the fund name is official SEC-registered nomenclature.

Case Study: JPMorgan Kinexys

Kinexys (formerly JPMorgan Onyx, rebranded 2024)

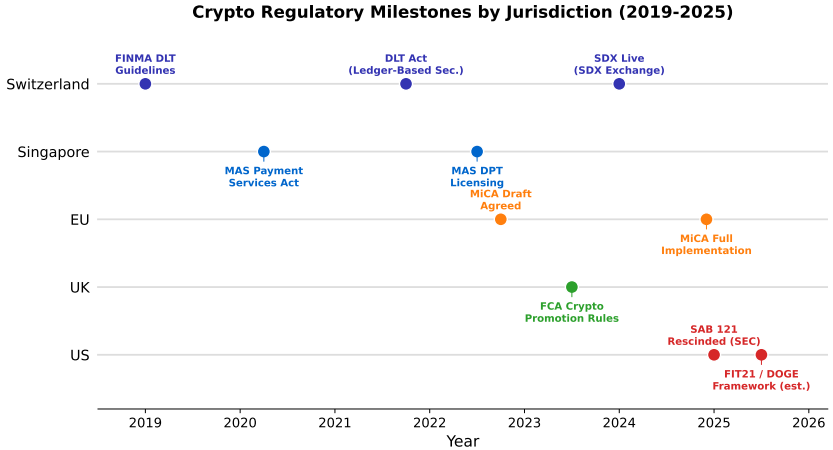
- JPM Coin (2019): first blockchain payment system by major US bank
- Kinexys Digital Payments: cross-border settlement in USD/EUR/GBP
- **Volume: $1B+ daily repo settlement** (2024) (Source: JPMorgan Kinexys reports, 2024)
- Kinexys Digital Assets: tokenised collateral (tri-party repo)
- Users: BlackRock, Barclays, BNY Mellon, Siemens
- Network: private Ethereum fork (Quorum lineage → ConsenSys)

Kinexys: What it proves

- Institutional blockchain can achieve real transaction volume at scale
- Intraday repo saves JPMorgan clients ∼$1M+/day in collateral costs (estimated)
- Private permissioned chain suits regulated entities
- Rebranding from "Onyx" signals product maturity

Kinexys processes intraday repo that was previously impossible (repo market closes at 3pm; blockchain settles 24/7).

Regulatory Landscape for Institutional Crypto



Note: Switzerland DLT Act (2021) enabled ledger-based securities. EU MiCA fully in force Dec 30, 2024. US framework remains fragmented; SAB 121 rescinded Feb 2025.

Switzerland's DLT Act (2021) created ledger-based securities as a new asset class. EU MiCA fully in force December 30, 2024. US framework remains fragmented.

Swiss Exercise: Pension Fund Digital Asset Decision

Scenario:

You are CIO of a CHF 2B Swiss occupational pension fund (*Pensionskasse*). The investment committee asks whether to allocate 1% (˜CHF 20M) to:

- **A** Bitcoin via a Swiss-domiciled ETP (SIX-listed)
- **B** BUIDL tokenised treasury fund (on-chain, USD-denominated)
- **C** Coinbase Institutional custody account (direct BTC)

Constraints to consider:

- FINMA regulatory perimeter for Pensionskassen
- BVV2 / OAK BV investment guidelines (diversification, asset categories)
- FX risk: CHF-base vs. USD-denominated assets
- Counterparty and custody requirements under Swiss law

Discussion questions (10 min)

1. Which option(s) fall within the BVV2/OAK BV "other investments" category, and what is the typical cap?
2. What due-diligence questions would FINMA expect your board to document?
3. How does each option handle the custody-segregation requirement for pension assets?
4. Which option would you recommend, and why?

BVV2 Art. 55 "other investments" category typically allows up to 15% of portfolio. Pension funds are supervised by BVG/LPP framework, not MiCA (which is EU-only).

Exercise Debrief: Swiss Pension Fund Analysis

Regulatory framework:

- FINMA supervises Swiss financial institutions, including Pensionskassen
- BVV2 (Verordnung über die berufliche Vorsorge) / OAK BV guidelines govern pension investments
- "Other investments" (BVV2 Art. 55): typically capped at 15%; crypto ETPs may qualify
- **Note**: MiCA is EU law: does **not** apply to Swiss pension funds

Option A (SIX ETP):

- Cleanest fit: exchange-traded, FINMA-regulated SIX venue
- Custody: ETP issuer (21Shares, WisdomTree) holds BTC in cold storage

Option B (BUIDL):

- USD FX risk; SEC-regulated (not FINMA primary)
- Custody: Coinbase (US-based); cross-border risk
- Novel asset class; board documentation burden high

Option C (Direct BTC):

- Requires detailed FINMA custody documentation
- Board likely needs external expert opinion
- Highest governance burden

Recommendation for most Pensionskassen (2024-2025): Option A, with full FINMA/BVV2 compliance documentation.

FINMA Circular 2018/3 (outsourcing) applies if custody is delegated. BVV2/OAK BV (not MiCA) governs Swiss pension asset allocation rules.

What TradFi Wants From Crypto Infrastructure

TradFi's requirements (non-negotiable):

- **Regulatory compliance**: licenced custodian, audited reserves, segregated assets
- **Insurance**: Lloyd's, Aon crypto custody policies (typically 1-5% AUC/year)
- **SLAs**: uptime guarantees, recovery-time objectives
- **Reporting**: GAAP/IFRS mark-to-market, tax lot tracking
- **Counterparty risk**: no self-custody, no exchange omnibus accounts

What crypto must provide:

- Proof of reserves (on-chain attestable)
- Institutional-grade API (FIX protocol, REST)
- AML/KYC-compliant token whitelisting
- Smart-contract audit and code escrow
- Legal enforceability of on-chain settlement

Gap closing: Coinbase, BitGo, Anchorage all now SOC 2 Type II certified and hold bank-equivalent licences in multiple jurisdictions.

SOC 2 Type II (security operations audit) and ISO 27001 have become baseline requirements for institutional crypto custodians.

Barriers to Institutional Adoption (Remaining)

Structural barriers:

- **Accounting treatment**: FASB ASC 350 updated 2023 (fair-value for crypto now allowed); IFRS still evolving
- **Capital charges**: Basel III crypto rules (Group 1/Group 2 classification); Group 2 (most crypto) = 1250% risk weight
- **Liquidity**: on-chain RWA markets thin vs. TradFi equivalents
- **Fragmentation**: no single settlement standard across chains

Regulatory/political barriers:

- **SAB 121** (US, 2022-2025): required banks to hold crypto on balance sheet at full cost; disincentivised custody; rescinded Feb 2025 (Source: SEC, Feb 2025)
- **AML/FATF Travel Rule**: token transfers >CHF 1000 require originator/beneficiary data
- **Tax uncertainty**: inconsistent treatment of staking income, DeFi yields, fork proceeds across jurisdictions

Direction: barriers falling; 2025-2027 likely sees significant institutional on-ramp acceleration.

Basel Group 2 crypto (1250% risk weight) makes holding Bitcoin on a bank balance sheet very expensive (driving ETF/fund structures). (Source: Basel Committee, Dec 2022)

The Future: Institutional DeFi

Permissioned DeFi ("CeDeFi"):

- KYC-whitelisted wallets only
- Smart contracts with regulatory compliance hooks
- Examples: Aave Arc (2022), Morpho Institutional, Centrifuge Prime

Canton Network (2023):

- Consortium of Goldman Sachs, BNY Mellon, Deloitte, Deutsche Boerse
- Privacy-preserving DeFi for institutional collateral
- Uses Daml smart contracts on Canton blockchain

Convergence thesis:

1. Tokenised RWAs become DeFi collateral
2. Institutional stablecoins replace wire transfers
3. On-chain identity (verifiable credentials) enables permissioned DeFi
4. AI agents manage multi-chain institutional portfolios

Timeline estimate: 5-10 years to significant TradFi/DeFi convergence.

"Institutional DeFi" is not an oxymoron: it is the next phase after tokenisation establishes the infrastructure layer.

Investment Products: Institutional Crypto Exposure

Regulated access channels:

- **Spot ETFs**: iShares Bitcoin Trust (IBIT), Fidelity Wise Origin: $60B+ AUM combined (as of 2025) (Source: Bloomberg ETF data, Jan 2025)
- **Futures ETFs**: ProShares BITO; basis roll cost applies
- **Tokenised funds**: BlackRock BUIDL ($2.9B), Franklin FOBXX; direct on-chain ownership
- **Regulated derivatives**: CME Bitcoin/Ether futures, cash-settled, no custody required

Why product structure matters:

- Spot ETF: pensionable asset class (BVV2/OAK BV: quantitative prudence test)
- Futures ETF: basis risk, roll cost erodes return vs. spot
- Tokenised fund: on-chain settlement, daily NAV, T+0 liquidity
- Direct custody: maximum exposure, maximum compliance burden

Trend: pension funds and SWFs prefer ETFs; hedge funds and crypto-native desks prefer direct custody.

The Bitcoin ETF (Jan 2024) was the institutional inflection point: it converted an "alternative" into a regulated, custodied product accessible via Bloomberg terminals.

The Economics of Institutional Crypto Infrastructure

Incentive structure:

- **Custodians** earn basis-point fees on AUC; quality custody commands 10-40 bp/year
- **Prime brokers** earn spread on OTC trades, interest on margin lending, staking commission
- **Tokenisation platforms** earn issuance fee + ongoing management fee (BUIDL: 0.5% p.a.)
- **Investors** gain yield, 24/7 liquidity, T+0 settlement

Value flow:

- Settlement efficiency savings: eliminate T+2 counterparty risk
- Collateral optimisation: intraday repo (Kinexys saves ∼$1M+/day client collateral costs)
- Yield: tokenised Treasuries on-chain earn same yield as off-chain but with DeFi composability

Security model: Custodian insurance, regulatory licence, and audit create reputation bond; rational not to misbehave.

The cryptoeconomics lens: institutional crypto solves the coordination problem of multi-party settlement by making misbehaviour costlier than honest participation.

Design Space: Institutional Crypto Infrastructure

Key design choices:

- **Permissioned vs. permissionless**: Kinexys (private) vs. BUIDL (public Ethereum), regulatory control vs. composability
- **MPC vs. HSM**: operational speed vs. hardware certainty
- **On-chain vs. off-chain NAV**: BUIDL accrues on-chain; FOBXX uses blockchain as registrar only
- **Custody model**: self-custody impossible for regulated entities; qualified custodian required (SEC Rule 17f-2)

Trade-offs examined:

- **Privacy vs. transparency**: permissioned chains preserve confidentiality; public chains enable auditability
- **Composability vs. compliance**: DeFi integration requires whitelisted wallets to avoid AML risk
- **Speed vs. finality**: fast settlement requires either trusted validator (centralisation) or long confirmation times

Alternative: keep everything off-chain with blockchain-mirrored record only (DTCC Digital Assets model).

No design dominates: the "right" architecture depends on regulatory jurisdiction, asset class, and counterparty set.

Failure Modes: Institutional Crypto Infrastructure

Assumptions that can fail:

- **Custodian honesty**: FTX held customer assets; lent them to Alameda; violated segregation
- **Smart contract correctness**: Euler Finance hack ($197M, 2023); even audited contracts fail
- **Regulatory stability**: SAB 121 changed custody economics overnight (2022-2025)
- **Key management**: exchange hacks total $3B+ in 2022 alone (Chainalysis)

Historical failures in institutional crypto:

- **Mt. Gox (2014)**: 850,000 BTC lost; inadequate key management
- **FTX (2022)**: commingled funds; no real segregated custody
- **Genesis/Gemini Earn (2023)**: prime lending without proper risk management
- **Silvergate / Signature Bank (2023)**: contagion from crypto-bank concentration

Warning sign: any custodian that cannot prove segregated, audited reserves in real time.

The lesson from FTX: "institutional grade" requires legal segregation, not just a slick dashboard. Proof of reserves must be cryptographically verifiable.

Key Takeaways

Custody and infrastructure:

- Hot/warm/cold storage: speed-security trade-off
- MPC (Multi-Party Computation): no single-point key failure
- HSM (Hardware Security Module): FIPS-certified tamper-proof hardware
- Leading custodians: Coinbase (∼$130B), BitGo (∼$64B), Fidelity (∼$50B)

Product ecosystem:

- Prime brokers bundle custody + trading + lending + derivatives
- Full-service platforms (Coinbase, Galaxy) closest to TradFi prime

Real-world asset tokenisation:

- $15B deployed on-chain (as of 2025); $4-16T addressable market
- BlackRock BUIDL: $2.9B (Dec 2024), largest tokenised fund
- Franklin FOBXX: first SEC-registered blockchain fund
- JPMorgan Kinexys: $1B+ daily repo volume

Institutional adoption drivers:

- Bitcoin ETF approvals (Jan 2024) opened pension/SWF access
- Spot Bitcoin ETFs (IBIT / FBTC): combined $60B+ AUM by Jan 2025; pensionable via BVV2/OAK BV
- Regulatory clarity (MiCA EU Dec 2024; Swiss DLT Act 2021) reduces compliance risk
- Basel III and SAB 121 repeal shaping bank participation

The shift from "crypto is unserious" to "BlackRock runs a $2.9B on-chain fund" happened in less than 5 years.

Further Reading & Data Sources

Market data:

- `rwa.xyz`: real-time RWA on-chain data
- `defillama.com`: DeFi TVL and institutional DeFi
- `21shares.com/research`: ETP market data
- Chainalysis Crypto Crime Report (annual)

Regulatory:

- FINMA Guidelines on Virtual Currencies (2018, updated)
- BVG/BVV2: Swiss pension investment framework
- Basel III crypto standard (Dec 2022 final)
- MiCA regulation text (EU): for EU-domiciled entities

Case studies:

- BlackRock BUIDL prospectus (SEC EDGAR)
- Franklin FOBXX Form N-1A (SEC EDGAR)
- JPMorgan Kinexys white papers (jpmorgan.com)
- SIX Digital Exchange annual report

Academic:

- Citi GPS: "Money, Tokens and Games" (2023)
- BCG / ADDX: "Relevance of On-Chain Asset Tokenization" (2022)
- BIS Working Paper No. 1065: "DeFi risks and the decentralisation illusion"

All market figures should be verified against live sources before use in research or investment decisions.